2014

Finding Zeros of Rational Quadratic Forms

John F. Shaughnessy
Claremont McKenna College

CLAREMONT MCKENNA COLLEGE

Finding Zeros of Rational Quadratic Forms

SUBMITTED TO

Professor Lenny Fukshansky
AND
Professor David Krumm

AND

Dean Nicholas Warner

BY

John Shaughnessy

for

SENIOR THESIS

Spring 2014

April 28th

Contents

FINDING ZEROS OF RATIONAL QUADRATIC FORMS

JOHN SHAUGHNESSY

Abstract. In this thesis, we introduce the notion of quadratic forms and provide motivation for their study. We begin by discussing Diophantine equations, the field of p-adic numbers, and the Hasse-Minkowski Theorem that allows us to use p-adic analysis to determine whether a quadratic form has a rational root. We then discuss search bounds and state Cassels' Theorem for small-height zeros of quadratic forms over $\mathbb{Q}$. We end with a proof of Cassels' Theorem and suggestions for further reading.

1. Introduction

To the uninitiated, those who pursue math appear to be doing little more than the calculation of equations using numbers, matrices, and geometric shapes. For those who see past its surface, however, the pursuit of proofs becomes a much more pleasurable and enlightening experience. Andrew Wiles, who in 1995 completed the proof of Fermat's Last Theorem after mathematicians sought the answer since 1637, said this of mathematics:

"Perhaps I can best describe my experience of doing mathematics in terms of a journey through a dark unexplored mansion. You enter the first room of the mansion and it's completely dark. You stumble around bumping into the furniture, but gradually you learn where each piece of furniture is. Finally, after six months or so, you find the light switch, you turn it on, and suddenly it's all illuminated. You can see exactly where you were. Then you move into the next room and spend another six months in the dark. So each of these breakthroughs, while sometimes they're momentary, sometimes over a period of a day or two, they are the culmination of (and couldn't exist without) the many months of stumbling around in the dark that precede them."

The purpose of this paper is to allow the curious undergraduate to step inside the mansion of quadratic forms and explore a few of its rooms. The reader is expected to know a bit about linear algebra, geometry, and in general feel comfortable reading and manipulating mathematical symbols. As this is intended to be a survey, however, the reader is encouraged to continue even if sections of the paper are incomprehensible to her at this time.

1.1. Polynomial Equations.

A Diophantine equation

$$F(x_1, x_2, \cdots, x_n) = 0$$

2010 *Mathematics Subject Classification.* Primary 11G50, 11E12, 11E39.
Key words and phrases. heights, quadratic forms.
The author was mentored by Lenny Fukshansky.

is a homogeneous polynomial equations in two or more unknowns with integer coefficients. When working with a Diophantine equation, we commonly ask:

Does it have any nontrivial solutions in integers? By nontrivial, we mean that $\vec{x} \neq 0$.
Are there finitely many integral solutions or infinitely many?
Is it theoretically possible to find all such solutions? How easy or difficult is it to do using computers?

Polynomial equations vary by the degree of their monomial terms. If all of the monomials are of the same degree, we say the polynomial is homogeneous and call it a form. Forms of degree 1, 2, 3, and 4 are called linear, quadratic, cubic, and quartic forms, respectively. In this paper we focus on quadratic forms, but the algebraic theory of quadratic forms extends well beyond what is presented in our limited scope.

For most of this paper, we will discuss equations with coefficients taken from $\mathbb{Q}$, as it is easier to solve equations over a field (where one may take inverses) than over the integers. We will also have to rely on an unfamiliar family of fields called the p-adic numbers.

1.1.1. *Diophantus.*

Diophantine equations have been studied since Diophantus of Alexandria introduced symbolism to algebra while studying such equations. Though his memory has been obfuscated by time, Diophantus contributed to mathematics by writing Arithmetica, a text in which he tried to solve 130 algebra problems. His interest in these types of equations paved the way for many mathematicians after him, not least of whom was Fermat.

1.1.2. *Fermat's Last Theorem.*

One particular Diophantine equation that shaped the course of mathematics is

$$x^n + y^n = z^n$$

where x, y, and z are all non-zero integers. When $n = 2$, integer solutions to this equation are Pythagorean triples, but for $n > 2$ it feels impossible to find a solution.

In 1637 French mathematician Pierre de Fermat wrote that he believed that none could be found. In the margins of his copy of *Arithmetica*, he claimed that he could prove it:

"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

But Fermat never wrote his marvelous proof. In fact, it is commonly believed that he could not have possessed a proof except for the case when $n = 4$ and perhaps for when $n = 3$. The answer did not come for over 300 years, during which time the search for a proof led to new areas of study that have become widely-explored branches of mathematics in their own right. In 1995, British mathematician Andrew Wiles provided the final piece of the puzzle and showed that when $n > 2$, no integral solutions to the equation $x^n + y^n = z^n$ exist (besides $x = y = z = 0$).

1.2. **How do we solve Diophantine equations?**

If no solution presents itself in an obvious way, it is difficult to know where to begin. If we exhaust ourselves by plugging in numbers by hand or on a computer,

we may begin to suspect that no solution exists. But how are we to decide that? This is the first task when solving a Diophantine equation - to determine whether it has a solution.

Helmut Hasse's local-to-global principle, introduced in 1921, can be applied as a means to determine whether a quadratic form had a solution or not. Cassels' Theorem provides a method (and algorithm) for finding nontrivial zeros of quadratic forms over $\mathbb{Q}$.

It is a common problem for a mathematician to know that a solution to a problem exists without having any idea how to find such a solution. Sometimes, we need to shift perspectives entirely before we can see our problem clearly. For Diophantine equations, we have invented a trick.

Given a single solution to a linear form, we can find infinitely more along the same line. When we generalize this principle, we find a way to translate our numerical perspective to a geometric perspective and try to attack the problem with geometric techniques. This switch lets us take advantage of both algebra and geometry. Thanks Hermann Minkowski's "Geometry of Numbers," a set of results from 1910, we may view the set of solutions of a quadratic form as a space or a shape and then analyze the geometry of such an object.

1.3. **Quadratic Forms.** An integral quadratic form is a homogeneous polynomial of degree 2. Thus, any quadratic form $f(x)$ can be written as

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} x_i x_j$$

where $f_{if} \in \mathbb{Z}$ for all $1 < i, j < N$.

There are numerous examples of quadratic forms, such as $x^2 + y^2 = n$ where n is an integer, which allows us to tell whether n is expressible as a sum of two square integers. In 1749, Euler showed that this equation has a solution if and only if no prime p that is equivalent to 3 (modulo 4) divides n to an odd power.

In Section 2 we build up our intuition by showing a few more examples and by presenting three equivalent ways to define a quadratic form.

1.4. **Hilbert's 10th Problem.**

In the year 1900, Hilbert announced and published 23 problems that helped shape the 20th century of mathematics. Of these, the 10th is our focus: *"Does there exist an algorithm to determine whether or not a Diophantine Equation has an integer solution¿'* Before we get to the answer, we try to understand the significance of such a question.

An **algorithm** is a terminating, deterministic procedure designed to carry out some function. In this case, Hilbert is asking whether such a sequence of steps could tell us if a solution existed for an arbitrary Diophantine Equation. In 1970, however, Matiyasevich famously proved that a general algorithm like this could not exist. For specific families of Diophantine Equations, however, the question is still more interesting.

1.5. **Search Bounds.**

Consider a system M of polynomials in multiple variables with integer coefficients:

$$P_1(x) = b_1$$

$$P_2(x) = b_2$$
$$\dots$$
$$P_M(x) = b_M.$$

Suppose we could prove that if this system has a solution, then a solution must exist with

$$|x|_{max} := \max_{1 \le i \le n} x_i \le C$$

for some constant C that depends on the coefficients. Since any compact set in $\mathbb{R}^n$ has finitely many integral points, we then reduce this problem to a trivial check of finitely many possibilities for the vector x. Such a constant C is called a *search bound*.

Much is known about search bounds for whole systems of linear forms, but we omit these results at the present and instead direct the curious reader to Bombieri and Vaaler's paper, "On Siegel's Lemma".

Suppose now that we have a single quadratic form:

$$f(x) = \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i X_j \in \mathbb{Z}[X].$$

Cassels' Theorem gives us an explicit search bound and hence provides a way to find zeros of the quadratic form over $\mathbb{Q}$. This will be the primary result of this paper, but first we will build up some machinery to get us there. This result has been generalized in a number of ways, and the last chapter will mention these generalizations and touch on a few open problems.

Little is known for cubic forms and it has been shown by J. P. Jones that whether a general Diophantine equation of degree four or larger has a solution in the positive integers is undecidable. Still less is known for (non-homogeneous) polynomials of degree four or larger.

1.6. **Overview of the Paper.**

This paper is intended to be accessible to any curious undergraduates with some exposure to Algebra and Geometry. Nothing presented here is beyond the scope of a simple Wikipedia search, so the reader is encouraged to look up the words she does not know and read until it makes sense. With that said, we will present the most relevant background information in Sections 2, 3, and 4.

1.6.1. *Quadratic Forms.*

Quadratic forms are homogeneous polynomials of degree 2, and they have been studied for a wide variety of reasons. For our purposes, we will give a few examples of quadratic forms and discuss multiple viewpoints from which we can approach the formal definition. When the quadratic form $f(\vec{x}) = 0$ has a nontrivial rational solution (one in which $\vec{x} \neq \vec{0}$), we say that f is isotropic over $\mathbb{Q}$.

1.6.2. *Absolute Values and p-adic Numbers.*

Although equations are solved most frequently over the integers ($\mathbb{Z}$), it was realized that equations are many times easier to solve when the coefficients are taken over a field (like $\mathbb{Q}$ or $\mathbb{R}$) rather than from $\mathbb{Z}$. Studying the properties of the familiar absolute value allows us to define an unfamiliar *completion* of the rationals called the p-adic numbers. By completing $\mathbb{Q}$ under this different notion

of "closeness", the p-adic numbers allow us to determine whether a quadratic form has a solution over $\mathbb{Q}$.

The Hasse-principle is a fascinating result that says that our form F is *isotropic* (has a nonzero solution) over $\mathbb{Q}$ if and only if it is isotropic over every completion of $\mathbb{Q}$ (namely the reals and the p-adics, due to a theorem of Ostrowski from 1916). This ineffective solution provides further insight into why Cassels' theorem is such a nice result.

1.6.3. *Search Bounds.*

Suppose we could prove that if a form has a nontrivial integral solution, then there must be an integral solution within a certain radius about the origin. Since it is often easier to prove that a form has a nontrivial zero than it is to find one specifically, this would be helpful in the search for a specific solution. If we knew the radius by which some solution is bounded, and we know that only finitely many integral points are within that radius, we've simplified the problem to one that we can solve with a computer in finite time. Furthermore, if the bounds we get on the size of our nontrivial zero are known, than we can tell whether a form has a solution by simply checking all the points within the bounds. Overall, this would be a powerful tool. In our case, this is precisely what Cassels' Theorem allows us to do:

Theorem 1.1 (Cassels' Theorem)**.** *Let*

$$f(\boldsymbol{x}) = \sum_{i=1}^{N}\sum_{j=1}^{N} f_{ij}x_i x_j \in \mathbb{Z}[\underline{x}]$$

be an isotropic integral quadratic form in $N \geq 2$ variables, then there exists $\boldsymbol{x} \in \mathbb{Z}^N \setminus \{\mathbf{0}\}$ such that $f(\boldsymbol{x}) = 0$ and

$$\max_{1\leq i\leq N} |x_i| \leq \left(3\sum_{i=1}^{N}\sum_{j=1}^{N} |f_{ij}|\right)^{\frac{N-1}{2}}. \tag{1}$$

2. Quadratic Forms

Quadratic Forms are the primary mathematical objects of our present study. We repeat the (standard) definition here. We say that F is an integral quadratic form if it is a homogeneous polynomial of degree 2 whose coefficients are taken in $\mathbb{Z}$:

$$f(x) = \sum_{i=1}^{N}\sum_{j=1}^{N} f_{ij}X_iX_j \in \mathbb{Z}[X].$$

We define a rational quadratic form similarly. Some sources define a form to be integral (or rational) if every solution is integral (or in $\mathbb{Q}$). The distinction is sometimes called being *classically integral* or *integer-valued*. Our forms will be classically integral (or classically rational).

2.1. **Examples of Quadratic Forms.**

The first obvious quadratic form one might be interested in is

$$f(x, y, z) = x^2 + y^2 - z^2.$$

Then solutions to the equation $f(x, y, z) = 0$ give the side-lengths of right-angled triangles. Hence if we find integral solutions, we are finding Pythagorean Triples. Note that we might also write this form as $f : \mathbb{Z} \to \mathbb{Z}$:

$$f(\vec{x}) = f(x_1, x_2, x_3) = (1)x_1^2 + (1)x_2^2 + (-1)x_3^2$$

to make it clear that the coefficients are (1,1,-1).

Another example of a quadratic form that has been of historical interest is

$$f(x, y, z) = x^2 + y^2 - 2z^2$$

which, when solved for $f(x, y, z) = 0$ yields the squares x^2, z^2, y^2 in arithmetic progression (i.e. $y^2 - z^2 = z^2 - x^2$).

Not all homogenous quadratic equations have integral solutions. Consider $x^2 + y^2 = -3$. Clearly there is no hope of finding a (rational) solution.

Sometimes, we are more interested in congruences than in equivalence. For example, any number squared is either 1 or 0 mod 4 ($x^2 = 0$ or 1 (mod 4) for all x). Hence if a is the sum of two squares then $a \not\equiv 3 \pmod 4$.

Although equations are solved most frequently over the integers ($\mathbb{Z}$), it was realized that equations are many times easier to solve when the coefficients are taken over a field (like $\mathbb{Q}$ or $\mathbb{R}$) rather than from $\mathbb{Z}$. With this in mind, we study Quadratic forms with $\mathbb{Q}$-coefficients as Minkowski and Hasse put forward in the 1880s and in 1921, respectively.

2.2. **Three Definitions of a Quadratic Form.**

We build some intuition about Quadratic Forms by giving three ways to think about them and show that each bears the same mathematical object.

Theorem 2.1 (Three ways to think about quadratic forms)**.** *For $n \in \mathbb{Z}^+$, there are canonical bijections between the following sets:*

(i) The set of homogeneous quadratic polynomials $q(t) = q(t_1, \cdots, t_n)$

(ii) The set of symmetric bilinear forms on $\mathbb{Q}^n$

(iii) The set of symmetric $n \times n$ matrices on $\mathbb{Q}^n$

Proof: To see how to get (ii) from (i), we prove that f_q has the following properties:

(a) For all $\alpha \in K$, $f_q(\alpha x) = \alpha^2 f_q(x)$.

(b) Let $B_f(x,y) := \frac{1}{2}(f_q(x+y) - f_q(x) - f_q(y))$. Then for all x, y, z in K^n and α in K
   (1) $B_f(x,y) = B_f(y,x)$
   (2) $B_f(\alpha x + y, z) = \alpha B_f(x,z) + B_f(y,z)$

We can prove (a) with a one-line proof:

$$f_q(\alpha x) = \sum_{1 \le i \le j \le n} a_{ij}(\alpha x_i)(\alpha x_j) = \sum_{1 \le i \le j \le n} \alpha^2 a_{ij}(x_i)(x_j) = \alpha^2 f_q(x)$$

To prove (b), all we need to do is expand via the definition of $B_f(x,y)$:

(1) The form is *symmetric*:

$$\begin{aligned} B_f(x,y) &= \frac{1}{2}(f_q(x+y) - f_q(x) - f_q(y)) \\ &= \frac{1}{2}(f_q(y,x) - f_q(y) - f_q(x)) \\ &= B_f(y,x) \end{aligned}$$

(2) The form is *bilinear*:

$$\begin{aligned} B_f(\alpha x + y, z) &= \frac{1}{2}(f_q(\alpha x + y + z) - f_q(\alpha x + y) - f_q(z)) \\ &= \frac{1}{2}(\alpha^2 f_q(x + z + y) - \alpha^2 f_q(x + y) - f_q(z)) \\ &= \alpha \frac{1}{2}(f_q(x+z) - f_q(z) - f_q(z)) + \frac{1}{2}(f_q(y+z) - f_q(y) - f_q(z)) \\ &= \alpha B_f(x,z) + B_f(y,z) \end{aligned}$$

Note that the bilinear form and the function determine one another, so that f_q and B_f carry the same information:

$$B_f(x,x) = \frac{1}{2}(f_q(2x) - 2f_q(x)) = \frac{1}{2}(4f_q(x) - 2f_q(x)) = f_q(x)$$

To see that (iii) follows from (ii), we notice that we may write the form

$$f(x) = \sum_{i=1}^{N} \sum_{j=1}^{N} f_{ij} X_i X_j \in \mathbb{Z}[X]$$

as $x^t \beta x$ where x^t is a column vector and β is the matrix of entries f_{ij}. Clearly β is symmetric since $f_{ij} = f_{ji}$. □

It is useful in many cases to switch from one mode of thinking to another while working with quadratic forms. For the purposes of this paper, we introduce this concept without exploring it in great detail. Instead, we navigate toward p-adic numbers in order to arrive at the Hasse-Minkowski theorem.

3. The p-adic Numbers

The p-adic number systems are extensions of $\mathbb{Q}$ that will allow us to determine whether a zero of a quadratic form exists in $\mathbb{Q}$ without having to find one specifically. We begin with basic operations on numbers represented in base p to build an intuition for a new notion of size (the p-adic valuation). We then sketch the construction of the p-adic numbers and contrast them with real numbers in an example. Lastly, we introduce Hensel's Lifting Lemma and end by stating the Hasse-Minkowski principle without proof.

3.1. **Rationals in Base p.**

Given a nonzero integer n and a prime p, we can write n in base p by using the unique set of integers, $a_0, \cdots, a_k$ with $0 \leq a_i < p$ for all i that satisfy

$$n = a_0 + a_1 p + a_2 p^2 + \cdots a_k p^k$$

and $a_k \neq 0$. We normally use the base 10 representation of integers. In other words, if $n = n_0 + n_1(10) + n_2(100) + \cdots + n_s(10^s)$ with $0 \leq n_i < 10$ for each i, we have

$$(n_s n_{s-1} \cdots n_1 n_0)_{(\text{Base } 10)} = (a_k a_{k-1} \cdots a_0)_{(\text{Base p})}.$$

We call $a_0, \cdots, a_k$ the p-adic digits of n.

We can extend this representation to the rationals. Let $\dfrac{u}{v} \in \mathbb{Q}$ where

$$u = u_0 + u_1 p + \cdots + u_k p^s$$

and

$$v = v_0 + v_1 p + \cdots + v_k p^t$$

in base p. We represent $\dfrac{u}{v}$ in the form

$$a_{-t} p^{-t} + a_{-(t-1)} p^{-(t-1)} + \cdots + a_{-1} p^{-1} + a_0 + a_1 p + a_2 p^2 + \cdots,$$

where we write $0 \cdot p^i$ whenever $u_i = v_i$ and $v_i p^{-i}$ whenever $u_i = 0$. There is no simply way to handle the case when $0 \neq u_i \neq v_i \neq 0$, and we must allow infinite expansion to the left in order to include all rationals. For the sake of simplicity, we will stick to integers for now.

If we want to add or subtract two integers in base p, the algorithm is the same as for integers in base 10:

$$\begin{array}{rcccl} & 1 & 2 & 3 & (\text{base } 7) \\ + & & 4 & 4 & (\text{base } 7) \\ \hline & 2 & 0 & 0 & (\text{base } 7) \end{array},$$

which is to say that

$$(1 * 7^2 + 2 * 7 + 3 * 1) + (4 * 7 + 4 * 1) = 2 * 7^2$$

and

$$\begin{array}{rcccl} & 1 & 2 & 3 & (\text{base } 7) \\ - & & 4 & 4 & (\text{base } 7) \\ \hline & 0 & 4 & 6 & (\text{base } 7) \end{array}$$

or

$$(1 * 7^2 + 2 * 7 + 3 * 1) - (4 * 7 + 4 * 1) = 4 * 7 + 6 * 1.$$

The same is true when we multiply by a rational or when we multiply two numbers in base 7:

$$\begin{array}{cccccccc} & & & & 1 & 2 & 3 & \text{(base 7)} \\ * & & & & & 4 & 4 & \text{(base 7)} \\ \hline & & & 1 & 1 & 2 & 5 & \text{(base 7)} \\ + & 1 & 1 & 2 & 5 & 0 & & \text{(base 7)} \\ \hline & 1 & 2 & 4 & 0 & 5 & & \text{(base 7).} \end{array}$$

There are some oddities for numbers written in base p. To show that division is not as straightforward as it is under normal representation, for instance, consider dividing 1 in half. This is the number $\frac{1}{2}$, but its base 7 representation is $\cdots 3334$ (with 3's repeating to the left), since twice this is $\cdots 001$, which is equal to 1. (If this is unclear, compare this to following the proof that $.999\cdots = 1$: Let $x = .999\cdots$. Then $10x = 9.999\cdots$ so that $9x = 9$. Hence $x = 1$.)

3.2. **Intuition.**

When thinking about the "size" of a rational number, it is natural to consider how many "steps away from zero" it is. Describing this as a function $||$ from the field $\mathbb{Q}$ to $\mathbb{R}_{\geq 0}$, is simple:

$$|x| = \begin{cases} x & \text{when } x \geq 0 \\ -x & \text{when } x < 0 \end{cases}$$

Objectively, however, there is no reason this ought to be the *only* way to think about size. And as we shall see, it's not.

3.3. **Absolute Values.**

The notion of size can be defined formally as an absolute value of a field. Concretely, given a field k, an absolute value on k is any function $|\ | : k \to \mathbb{R}_{\geq 0}$ that satisfies the following properties:

$$(1)\ |x| = 0 \text{ if and only if } x = 0$$

$$(2)\ |xy| = |x||y| \text{ for all } x \text{ and } y \text{ in } k$$

$$(3)\ |x + y| \leq |x| + |y| \text{ for all } x \text{ and } y \text{ in } k$$

It easy to see that the usual absolute value on Q satisfies these three conditions. A fourth condition that some absolute values maintain is

$$(4)\ |x + y| \leq \max\{|x|, |y|\} \text{ for all } x \text{ and } y \text{ in } k,$$

which is a stronger condition than (3). (In other words, (4) $\implies$ (3).)

An absolute value that satisfies condition (4) is said to be a **non-archimedean** absolute value. Otherwise, it is **archimedean**. It is easy to see that the trivial absolute value,

$$|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise} \end{cases}$$

is non-archimedian. Notice that since any nonzero element of a finite field can be raised to some power to yield 1, the trivial absolute value is the only possible absolute value on a finite field.

3.4. **p-adic Valuation.**

We are now ready to understand a p-adic valuation, which we will use in the definition of a p-adic absolute value. Let p be a prime number. The p-adic valuation is the function $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{R}$ defined as follows:

$$n = p^{v_p(n)} n' \text{ with } p \not| n'$$

In other words, the valuation v_p of a number n is the highest power of p that divides n. For example $v_3(18) = 2$ since $18 = 3^2 * 2$. We extend this valuation to $\mathbb{Q}$ by defining $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.

The following lemma captures two basic properties of the valuation:

3.4.1. *Lemma.*

(i) $v_p(xy) = v_p(x) + v_p(y)$.
(ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$ (when we define $v_p(0) = \infty$).

Proof: First, (i) is obvious because

$$v_p(xy) = p^{v_p(x)} x' * p^{v_p(y)} y' = p^{v_p(x)+v_p(y)} * x'y'$$

with $p \nmid x'y'$. Next, we leave (ii) to the reader and suggest factoring out common powers of p.

Notice that (i) is similar to condition (2) of absolute values except that a product has been replaced by the sum. Also, (ii) is related to property (4) (the non-archimedean replacement of the triangle inequality) in an odd way. Before continuing, can you guess what to do with v_p in order to define a non-archimedean absolute value on $\mathbb{Q}$? (Hint: Think about the rules of exponents and logarithms.)

3.5. **p-adic Absolute Value.**

We now define the p-adic absolute value and use it to hand-wave our way to the p-adic numbers.

3.5.1. *p-adic Absolute Value.* Let x be a rational number and p, a prime. Then the p-adic absolute value of x is defined to be

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

It is easy to check that $|\ |_p$ is a non-archimedean absolute value on $\mathbb{Q}$, as it follows from the lemma. We compute some examples over $\mathbb{Q}$ with $p = 7$:

$$|35|_7 = 7^{-1} = \frac{1}{7}$$

$$\left|\frac{56}{12}\right|_7 = 7^{-(v_7(56)-v_7(12))} = 7^{-(1-0)} = \frac{1}{7}$$

$$|177553|_7 = 1$$

$$\left|\frac{3}{686}\right|_7 = 343$$

Notice that our intuition for whether one number is "larger" than another (35 versus $\frac{3}{686}$) will lead us astray.

3.6. p-adic Completion of $\mathbb{Q}$.

We sketch the construction of the p-adic numbers. For a more complete description of this construction, see Gouvêa's *p-adic Numbers: An Introduction*.

Let C be the set of all Cauchy sequences in $\mathbb{Q}$ with respect to a particular p-adic absolute value. Then if (a) and (b) are elements of C, we can define the operations $+$ and $*$ on C pairwise to give C a ring structure:

$$(a) + (b) = (a_1 + b_1, a_2 + b_2, \cdots)$$

$$(a)(b) = (a_1 b_1, a_2 b_2, \cdots).$$

Next, let $S = \{c \in C : \lim_{n\to\infty}(c) \to 0\}$ be the set of all sequences whose limit is 0. This set turns out to be a maximal ideal in C, so that the quotient group C/S is a field. We call C/S the p-adic numbers, and use the notation $\mathbb{Q}_p$. Although we do not do so presently, the next steps involve showing that $\mathbb{Q}_p$ is complete and that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

We can extend the p-adic absolute value on $\mathbb{Q}$ to $\mathbb{Q}_p$ by defining the p-adic absolute value of $x \in \mathbb{Q}_p$ as the limit of the sequence $(|x_1|_p, |x_2|_p, \cdots)$. Note that if $u \in \mathbb{Q}$, the sequence $(u, u, \cdots)$ is also in $\mathbb{Q}_p$, so that $\mathbb{Q}$ and $\mathbb{Z}$ are embedded in $\mathbb{Q}_p$.

Next we define the p-adic integers, $\mathbb{Z}_p$, to be those elements of $\mathbb{Q}_p$ whose absolute value is bounded by 1:

$$\mathbb{Z} := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

In particular, these are all of the elements of $\mathbb{Q}_p$ that converge to a number whose base p representation has no p-adic digits after the dot. A regular integer always has a finite number of digits to the left of the dot and only 0's to the right. An element of $\mathbb{Z}_p$ may have a non-terminating sequence of digits to the left of the dot, but still has only 0's to the right.

We now look at a surprising difference between $\mathbb{R}$ (otherwise known as Q_∞ for historical reasons) and $\mathbb{Q}_p$.

3.7. Surprisingly Convergent Series in $\mathbb{Z}_p$.

In calculus we had a variety of tests to tell whether a series converges in $\mathbb{R}$. We will show that the infinite series $1 + p + p^2 + \cdots$ (which clearly diverges in $\mathbb{R}$) converges in Q_p.

First, let us recall the definition of a Cauchy sequence. A sequence of numbers is called a Cauchy sequence if for any $\epsilon > 0$ there exists an N such that $n \geq N$ implies $|s_n - s_{n+k}| < \epsilon$ for all k. Notice that here $|\ |$ can mean $|\ |_\infty$ when we are in $\mathbb{R}$ and $|\ |_p$ when we are in Q_p.

The series $1 + p + p^2 + \cdots$ can be thought of as the limit (should one exist) of the partial sums

$$s_n = 1 + p^1 + \cdots + p^{n-1} = \frac{1 - p^n}{1 - p}.$$

At this point, $1 - p^n$ diverges in the reals but goes to zero with respect to the p-adic absolute value since

$$|p^n|_\infty = p^n \to \infty$$

but

$$|p^n|_p = p^{-n} \to 0$$

as n tends to ∞. Hence not only does the sequence $1 + p + p^2 + \cdots$ converge in $\mathbb{Q}_p$ but it even converges to the rational number $\dfrac{1}{1 - p}$.

3.8. **Hensel's Lemma.**

Hensel's Lifting Lemma is one of the most important results when using p-adic numbers. Essentially, Hensel's Lemma gives you a method to test whether a polynomial has roots in $\mathbb{Z}_p$ (the p-adic integers). We state the Lemma without its proof:

Theorem 3.1 (Hensel's Lemma)**.** *If $f(x) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Z}_p[X]$ and there exists an $a \in \mathbb{Z}_p$ such that*

$$f(a) \equiv 0 \text{ (mod } p\text{), and } f'(a) \not\equiv 0 \text{ (mod } p\text{),}$$

then there exists a unique p-adic integer $b \in \mathbb{Z}_p$ with $f(b) = 0$ and $b \equiv a$ (mod p).

Hensel's Lemma is a powerful result. It is a fundamental tool in p-adic analysis and makes many problems simpler than they would be with real analysis.

3.8.1. *Hensel's Lemma and Quadratic Reciprocity.*

We can use our knowledge of Hensel's Lemma and of quadratic reciprocity to tell whether a given number n has a root in $\mathbb{Z}_p$. Let p be an odd prime and n be an integer such that $p \nmid n$. First we look at the equation

$$x^2 - n = 0$$

considered in $\mathbb{Z}_p[x]$. We reduce this to get

$$x^2 - n' \equiv 0 \text{ (mod p)}$$

considered in $\mathbb{F}_p[x]$ with $0 \leq n' < p$.

This has a solution if n' is a square (mod p), so that we have reduced the problem to one that we know how to solve. If by using the Legendre symbol $\left(\frac{n'}{p}\right)$ we find that n' is not a square (mod p), then we are done and can conclude that

$$x^2 - n = 0$$

considered in $\mathbb{Z}_p[x]$ has no solution.

If on the other hand we find that n' is a square (mod p), we need to find out whether the root to the equation is simple or not by taking the derivative. Doing so yields

$$2x \equiv 0 \text{ (mod p)}$$

which has only the trivial root, 0. Hence n is a square in Z_p if and only if it is a square (mod p).

We do an example to illustrate this process. Suppose we were given the equation $x^2 + 5 = 0$ and were asked to find a p such that it has a solution in $\mathbb{Z}_p$. This is the case if and only if $x^2 \equiv -5$ (mod p) has a simple root. In other words, we need a p with $\left(\frac{p-5}{p}\right) = 1$. We try $p = 23$ (so that $p - 5 = 18$) and we get

$$\left(\frac{18}{23}\right) = \left(\frac{3}{23}\right)^2 \left(\frac{2}{23}\right) = \left(\frac{2}{23}\right) = 1.$$

Hence 18 is a square (mod 23), which means that there exists a solution to the relation $x^2 \equiv -5$ (mod 23). Furthermore, we know that the equation $x^2 \equiv -5$ (mod 23) has a simple root since the only solution to $2x \equiv 0$ (mod 23) is 0 (mod 23). By Hensel's Lemma we can conclude that the root lifts; that is, there must exist a solution to $x^2 + 5 = 0$ in $\mathbb{Z}_{23}$.

Finally we are ready to connect our exploration of p-adic numbers back to the topic at hand: their involvement in the theory of quadratic forms.

3.9. **Local to Global Principle.**

The idea behind the Local-Global principle is that we can study solutions in $\mathbb{Q}$ (called *global solutions*) of Diophantine equations by observing whether the equation has solutions in $\mathbb{Q}_p$ (*local solutions*). This is not the case for all Diophantine equations, but the Hasse-Minkowski theorem is a miraculous case where the principle holds.

Theorem 3.2. *Hasse-Minkowski Theorem Let $F(X_1, X_2, \cdots, X_n) \in \mathbb{Q}[X_1, X_2, \cdots, X_n]$ be a quadratic form. The equation $F(X_1, X_2, \cdots, X_n) = 0$ has nontrivial solutions in $\mathbb{Q}$* ***if and only if*** *it has nontrivial solutions in $\mathbb{Q}_p$ for each $p \leq \infty$.*

This theorem helps us find out whether a rational solution exists, but it does not provide a method of finding such a solution.

4. Cassels' Theorem

In the previous section, we found that the Hasse-Minkowski theorem allows us to use p-adic analysis to find out whether a quadratic form is isotropic over $\mathbb{Q}$ - that is, whether it has a nontrivial, rational zero. Next, we introduce Cassels' Theorem so that we may find a zero that is not "too big".

Cassels' Theorem states that if f is isotropic in $\mathbb{Z}[x_1, \cdots, x_n]$ then it must have a nontrivial zero whose absolute value is bounded by a constant. The bound given by Cassels' Theorem is called a *search bound*, as it lets us search through finitely many integer points (those who absolute value is less than the bound) in order to find a zero of small height.

The search bound given by Cassels' Theorem has been improved for forms over different fields or with special properties. It has also been generalized to accommodate new notions of height and absolute value, but for our purposes we stick to a proof using the absolute value

$$|\ | : \mathbb{Z}^n \to \mathbb{R}, |\vec{a}| = \max_{1 \le i \le n} |\vec{a_i}|$$

In order to prove Cassels' Theorem, we need to borrow a few ideas from the Geometry of Numbers, an approach to number theory studied most effectively by Minkowski, his pupil Hasse, and later by Witt. Here, we rely only on Minkowski's Linear Forms Theorem and a corollary.

4.1. **Minkowski's Linear Forms Theorem.**

By now the reader ought to be familiar with a quadratic form as a homogeneous polynomial of degree 2. A *linear* form, on the other hand, is simply a homogeneous polynomial of degree 1. Minkowski's Linear Forms Theorem allows us to find a non-zero $\vec{a} \in \mathbb{Z}^n$ such that the height of the form at $\vec{a}$ is bounded (essentially) by the determinant of the form. We state the theorem without proof:

Theorem 4.1 (Minkowski's Linear Forms Theorem)**.** *Let $L_j(x)$ $(1 \le j \le n)$ be real linear forms in n variables (i.e. $\vec{x} = (x_1, \cdots, x_n)$) with determinant $D \neq 0$. Let $t_j > 0$ $(1 \le j \le n)$ satisfy*

$$t_1 \cdots t_n \ge |D|. \tag{2}$$

Then there is a non-zero $\vec{a} \in \mathbb{Z}^n$ such that

$$|L_1(\vec{a})| \le t_1 \tag{3}$$

and

$$|L_j(\vec{a})| < t_j| \text{ for } (2 \le j \le n). \tag{4}$$

We record a useful corollary to the theorem.

Corollary 4.2. *Let $n \ge 1$, $M > 1$ be integers and let $\theta_1, \cdots, \theta_n$ be real numbers. Then there is an integer m in $0 < m < M$ and integers $l_1, \cdots, l_n$ such that*

$$|m\theta_j - l_j| \le M^{-\frac{1}{n}} = \frac{1}{\sqrt[n]{M}}$$

We will take advantage of the corollary when we prove Cassels' Theorem.

4.2. **Cassels' Theorem.**

Hilbert's 10th problem is one of *decidability*: it asks whether an algorithm to solve Diophantine equations *could* exist. In the case of quadratic forms, Cassels' Theorem gives us an effective solution - that is, provides us an explicit algorithm. It allows us to place an upper bound on the size of an integral solution should one exist, which reduces our problem of finding a zero to a process of checking finitely many possibilities. Since we can find the bound by summing the coefficients, our algorithm is simply one that checks every integral point less than the bound.

We are now ready to prove our main result.

Theorem 4.3 (Cassels' Theorem)**.** *Let*

$$f(x) = \sum f_{ij} x_i x_j \in \mathbb{Z}[x_1, \cdots, x_n] \tag{5}$$

be an isotropic form in n variables. Then there is an

$$\vec{a} \in \mathbb{Z}^n, \vec{a} \neq \vec{0} \tag{6}$$

with

$$f(\vec{a}) = 0 \tag{7}$$

such that

$$\max_{1 \leq j \leq n} |a_j| \leq (3F)^{\frac{n-1}{2}} \tag{8}$$

where

$$F = \sum_{i,j} |f_{ij}| \tag{9}$$

Here | | denotes the absolute value.

Since the proof is lengthy, we provide a few words about the way it works. (1) We begin by setting $\vec{a}$ to be the smallest solution to the form. (2) We then use the corollary above to construct a point $\vec{b}$ that is definitely not zero and definitely not a solution. (3) A clever linear combination of $\vec{a}$ and $\vec{b}$ gives us a point $\vec{a}^*$ that is another solution to the form. (4) Finally, we show that we can bound the size of $\vec{a}^*$ such that $||\vec{a}^*|| \leq 3F^{\frac{n-1}{2}}$. Since $\vec{a} \leq \vec{a}^*$, this completes the proof. The defining idea behind the proof is geometric in nature: the point $\vec{a}^*$ is a reflection of $\vec{a}$ over the hyperplane orthogonal to $\vec{b}$, where orthogonality is with respect to the symmetric bilinear form f.

Proof:

(1) Since f is isotropic, it has at least one nontrivial solution. We let $\vec{a}$ be the solution whose absolute value $||\vec{a}|| = \max_{1 \leq j \leq n} |a_j|$ is minimal. In other words, we start with the smallest vector $\vec{a}$ with respect to the absolute value on $\mathbb{Z}^n$ that associates to each vector its largest coordinate (in the Euclidean sense).

If $||\vec{a}|| > (3F)^{\frac{n-1}{2}}$ then we are going to find a different vector, $\vec{a}^*$ for which $f(\vec{a}^*) = 0$ (it is a solution) and $||\vec{a}^*|| < ||\vec{a}||$, which will contradict the minimality of $\vec{a}$.

To simplify our thinking, it will help if a_1, the first coordinate of $\vec{a}$, is both positive and equal to $||\vec{a}||$ (which means that $a_1 \geq a_i$ for $2 \leq i \leq n$). We may have to permute the indices of $\vec{a}$ and take $-\vec{a}$ instead of $\vec{a}$ in order for this condition to hold. This does not change the problem because $f(\vec{a}) = f(-\vec{a}) = 0$ and the order of indices is arbitrary.

As a final simplifying step, we note that there is nothing to prove if $a_1 = 1$, so we may suppose that $a_1 \geq 2$.

(2) If $\theta_1, \cdots, \theta_n$ are any real numbers, then (by the corollary above) there exists integers $b_1, \cdots, b_n$ such that $0 < b_1 < a_1$ and

$$|b_1\theta - b_j| \leq a_1^{\frac{-1}{(n-1)}}$$

for $(2 \leq j \leq n)$. If we set $\theta_j = \dfrac{a_j}{a_1}$ then by the triangle inequality we have

$$|b_j| \leq |b_1\theta_j| + a_1^{\frac{-1}{n-1}} \leq b_1 + a_1^{\frac{-1}{n-1}} \leq b_1 + 1$$

so that $\vec{b}$ has absolute value strictly less than $\vec{a}$:

$$||\vec{b}|| = \max_j |b_j| = b_1 < ||\vec{a}||.$$

We know that $\vec{b}$ is not zero because we chose $0 < b_1 < a_1$ and we know that it cannot be a solution to the equation because it would contradict the minimality of $||\vec{a}||$. Hence $f(b) \neq 0$.

(3) Now we take a clever linear combination of $\vec{a}$ and $\vec{b}$ to get a vector $\vec{a}^*$. Let $\vec{a}^* = \lambda\vec{a} + \mu\vec{b}$ where $\lambda = f(\vec{b}) \in \mathbb{Z}(\neq 0)$ and $\mu = -2f(\vec{a}, \vec{b}) \in \mathbb{Z}$.

The first thing we show about $\vec{a}^*$ is that $f(\vec{a}^*) = 0$:

$$\begin{aligned} f(\vec{a}^*) &= f(\lambda\vec{a} + \mu\vec{b}) \\ &= \lambda^2 f(\vec{a}) + 2\lambda\mu f(\vec{a}, \vec{b}) + \mu^2 f(\vec{b}) \\ &= 2\lambda\mu f(\vec{a}, \vec{b}) + \mu^2 f(\vec{b}) \\ &= 2(f(\vec{b}))(-2f(\vec{a}, \vec{b}))f(\vec{a}, \vec{b}) + (-2f(\vec{a}, \vec{b}))^2 f(\vec{b}) \\ &= -4f(\vec{a}, \vec{b})^2 f(\vec{b}) + 4f(\vec{a}, \vec{b})^2 f(\vec{b}) \\ &= 0 \end{aligned}$$

So that $\vec{a}^*$ is a solution.

Next, we know that $\vec{a}^* \neq 0$ because its definition, $\vec{a}^* = f(\vec{b})\vec{a} - 2f(\vec{a}, \vec{b})\vec{b}$ would then imply that $f(\vec{b}) = f(\vec{a}) = 0$, which is a contradiction to the fact that $f(\vec{b}) \neq 0$.

We have found a nonzero solution to the form, which means that by the minimality of $||\vec{a}||$,

$$||\vec{a}|| \leq ||\vec{a}^*||.$$

The final thing we must do is bound the absolute value of $\vec{a}^*$. That is, we must show

$$||\vec{a}^*|| \leq (3F)^{\frac{n-1}{2}}.$$

(4) We want to express $\vec{a}^*$ in a way that will allow us to approximate the size of $\vec{a}^*$ by comparing it only to the size of $\vec{a}$. We will do so by writing the coordinates of $\vec{b}$ as

$$b_j = \phi a_j + \delta_j$$

where where $\phi = \frac{b_1}{a_1}$, $d_1 = 0$, and $|d_j| \leq a_1^{\frac{-1}{n-1}}$ for all $(2 \leq j \leq n)$. Hence $\vec{b} = \phi\vec{a} + \vec{\delta}$.

We observe that

$$\begin{aligned} f(\vec{a},\vec{b}) &= f(\vec{a},\phi\vec{a}+\vec{\delta}) \\ &= \phi f(\vec{a}) + f(\vec{a},\vec{\delta}) \\ &= f(\vec{a},\vec{\delta}), \end{aligned}$$

and that

$$\begin{aligned} f(\vec{b}) &= f(\phi\vec{a}+\vec{\delta}) \\ &= 2\phi f(\vec{a}+\vec{\delta}) + f(\vec{\delta}). \end{aligned}$$

Using this, we can write

$$\begin{aligned} \vec{a}^* &= f(\vec{b})\vec{a} - 2f(\vec{a},\vec{b})\vec{b} \\ &= f(\phi\vec{a}+\vec{\delta})\vec{a} - 2f(\vec{a},\phi\vec{a}+\vec{\delta})(\phi\vec{a}+\vec{\delta}) \\ &= f(\vec{\delta})\vec{a} - f(\vec{a},\vec{\delta})\vec{\delta}. \end{aligned}$$

In this form, crude estimation is enough to show

$$||\vec{a}^*|| \leq 3F||\vec{a}||||\vec{\delta}||^2.$$

Since $||\vec{a}||$ is minimal, $||\vec{a}^*|| \geq ||\vec{a}||$ and $3F||\vec{\delta}||^2 \geq 1$. But since we defined $\vec{\delta}$ with $d_1 = 0$ and $|d_j| \leq a_1^{\frac{-1}{n-1}}$ for all $(2 \leq j \leq n)$, we have

$$||\vec{\delta}|| \leq a_1^{\frac{-1}{n-1}} = ||\vec{a}||^{\frac{-1}{n-1}}.$$

Hence $||\vec{a}|| \leq (3F)^{\frac{n-1}{2}}$, as we desired to show.

This concludes the proof of Cassels' Theorem. This proof is essentially the same as the one Cassels' gives in his *Quadratic Forms Over The Rationals* (Chapter 6).

5. Conclusion

Quadratic forms are a particularly interesting set of polynomials, and we have discussed a method to finding zeros of a quadratic form f. The Hasse-Minkowski theorem tells us that the quadratic equation $f(x) = 0$ will have a global solution (a root in $\mathbb{Q}$) if and only if it has solutions in every local field (in $\mathbb{Q}_p$ for all primes p and in $\mathbb{R}$). This fact is not at all true for most forms, but the quadratic case is a special one. If we know f is isotropic over $\mathbb{Q}$, then Cassels' theorem provides us with an explicit search bound within which a root can definitely be found.

Cassels' theorem is the first of many explicit search bounds found over fields. For particular quadratic forms, our search algorithm for rational or integral solutions can be improved. Cassels' theorem is very interesting in that it applies a geometric argument to accomplish its goals, making use of the geometry of numbers put forth by Minkowski, Hasse, and Witt. If the reader is interested in the same result over a field different from rationals, L. Fukshansky's paper *Heights and quadratic forms: Cassels' theorem and its generalizations* is a great resource.

5.1. **Further Reading.**

A more thorough discussion of the topics mentioned here, as well as many other interesting topics, can be found in J.W.S. Cassels' *Rational Quadratic Forms*. Another great resource for general information on Quadratic Forms and Bilinear Algebra is K. Szymiczek's *Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms*. In it, Szymiczek explains everything from the basics of bilinear spaces to Witt's results (Decomposition Theorem, Witt's invariant, Witt ring) and beyond. Denis Simon's paper listed in the section below provides an algorithm to efficiently solve any general ternary quadratic equation over $\mathbb{Q}$.

For a friendly introduction to p-adic numbers, consider Gouvêa's *p-adic Numbers: An Introduction*. This is a great resource for self study and is accessible to intermediate undergraduate math students.

We provide a list of resources that have been used in preparation of this thesis, as well as suggestions for further reading in the references section below.

5.2. **Acknowledgements.**

I would like to thank Professor Lenny Fukshansky for his academic guidance and patient mentorship. I would also like to thank Professor David Krumm for his generous feedback and useful suggestions as well as Professor Asuman Aksoy, whose words of encouragement facilitated my exploration of Mathematics.

References

[1] Quadratic form. Encyclopedia of Mathematics. http://www.encyclopediaofmath.org/index.php?title=Quadratic_form&oldid=24119.

[2] Bombieri, E. and Vaaler, J. "On Siegel's lemma". Invent. Math. 73 (1983), no. 1, 11?32

[3] J. W. S. Cassels. Bounds for the least solutions of homogeneous quadratic equations. *Proc. Cambridge Philos. Soc.*, 51:262–264, 1955.

[4] J. W. S. Cassels. *Rational quadratic forms*. Academic Press, Inc., 1978.

[5] P. L. Clark. Quadratic Forms Chapter 1: Witt's Theory. http://math.uga.edu/~pete/quadraticforms.pdf.

[6] L. Fukshansky. Heights and quadratic forms: on Cassels' theorem and its generalizations. In W. K. Chan, L. Fukshansky, R. Schulze-Pillot, and J. D. Vaaler, editors, *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, Contemp. Math., 587, pages 77–94. Amer. Math. Soc., Providence, RI, 2013.

[7] F. Q. Gouvêa. *p-adic numbers. An introduction. Second edition*. Universitext. Springer-Verlag, Berlin, 1997.

[8] J. P. Jones. Undecidable diophantine equations. *Bull. Amer. Math. Soc. (N.S.)*, 3(2):859–862, 1980.

[9] Y. Kitaoka. *Arithmetic of Quadratic Forms*. Cambridge University Press, 1993.

[10] D. W. Masser. Search bounds for Diophantine equations. *A panorama of number theory or the view from Baker's garden (Zurich, 1999)*, pages 247–259, 2002.

[11] Yu. V. Matijasevich. The diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[12] O. T. O'Meara. *Introduction to quadratic forms*. Springer-Verlag, 1973.

[13] W. Scharlau. *Quadratic and Hermitian Forms*. Springer-Verlag, 1985.

[14] J.-P. Serre. *A Course in Arithmetic*. New York: Springer, 1993.

[15] C. L. Siegel, K. Chandrasekharan, and R. Suter. *Lectures on the Geometry of Numbers*. Berlin: Springer-Verlag, 1989.

[16] Simon, Denis. "Solving Quadratic Equations Using Reduced Unimodular Quadratic Forms." *Mathematics of Computation 74.251 (2005): 1531-544. Print.*

[17] K. Szymiczek. Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms. *Amsterdam, the Netherlands: Gordon and Breach Science, 1997.*

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711

E-mail address: jshaughnessy14@cmc.edu